

IN THE CLAIMS

The entire pending claim set is provided for the Examiner's convenience. A marked-up version of the claims is provided in Appendix A attached to this document.

Please amend claims 1-8 as follows.

1        1. (Amended) A method for providing connection security for the  
2        transmission between communicating parties in a telecommunication network, the  
3        method comprising the steps of:  
4                exchanging security parameters between communicating parties,  
5                providing connection security for messages based on these security  
6        parameters,  
7                transmitting said messages between communicating parties,  
8        wherein the method further comprises the steps of:  
9                reaching agreement between communicating parties on an interval for  
10      recalculating of the security parameters,  
11                monitoring of the interval for recalculating by the communicating parties,  
12                recalculating the security parameters at the agreed interval, and  
13                providing connection security for messages based on the latest recalculated security  
14        parameters.

1        2. (Amended) The method according to claim 1, wherein providing  
2        connection security for messages based on the latest recalculated security parameters  
3        comprises the step of  
4                ciphering messages based on the latest recalculated security parameters.

1           3. (Amended) The method according to claim 1, wherein providing  
2 connection security for messages based on the latest recalculated security parameters  
3 comprises the step of  
4           authenticating and providing integrity for the messages based on the latest  
5 recalculated security parameters.

1           4. (Amended) The method according to claim 1, wherein providing  
2 connection security for messages based on the latest recalculated security parameters  
3 comprises the steps of  
4           ciphering messages based on the latest recalculated security parameters, and  
5           authenticating and providing integrity for the messages based on the latest  
6 recalculated security parameters.

*B1  
CONT.*

1           5. (Amended Twice) The method according to claim 3, wherein  
2 authenticating and providing integrity for the messages is arranged with a message  
3 authentication code MAC.

1           6. (Amended) The method according to claim 1, wherein the method  
2 further comprises the steps of:  
3           numbering the messages,  
4           agreeing on the number of messages to determine the interval for the  
5           recalculation of the security parameters,  
6           recalculating the security parameters after the agreed number of messages  
7           have been transmitted.

1           7. (Amended) The method according to claim 6, wherein the method  
2 further comprises the steps of:  
3           numbering the messages with sequence numbers,  
4           transmitting the sequence number with the message, and  
5           using the latest sequence number as input for recalculation of the security  
6 parameters.

*B1 Cncl'*  
1           8. (Amended) The method according to claim 1, wherein the method  
2 comprises the step of  
3           reaching agreement between communicating parties during handshaking on the  
4 interval for recalculation of the security parameters.

---